Distributed Trust Management; Exam 17/4/2012

Questions

1. **(1.5 points)** Let TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED be the security levels (ordered from highest to lowest) and Nuclear and Army be two categories. We have four subjects:

   - the president has TOP SECRET clearance for Nuclear and Army,
   - the colonel has SECRET clearance for Army and Nuclear,
   - the major has only CONFIDENTIAL clearance for Army, and
   - the soldier has only UNCLASSIFIED clearance for Nuclear.

   We also have some objects (documents):

   - the army position at security level SECRET,
   - the number of army units at security level CONFIDENTIAL,
   - the number of nuclear units at security level CONFIDENTIAL,
   - the costs of the nuclear program at security level UNCLASSIFIED,
   - the costs of the army at security level UNCLASSIFIED, and
   - the nuclear code at security level TOP SECRET.

   Answer the following questions based on the Bell-LaPadula model:

   (a) Draw the lattice of classifications.
   (b) Can the president compute the overall defense costs (army + nuclear)?
   (c) Can the major compute the total number of nuclear and army units?
   (d) Can the colonel compute the total number of nuclear and army units?
   (e) Can the colonel change the army position?
   (f) Can the major change the nuclear code?
   (g) Can the soldier change the nuclear code?

   Justify the answers.

2. **(1 points)** Describe the Bell-LaPadula and Biba models and how these two models can be combined.

3. **(1.5 points)** Write a UCON policy supporting the following scenario.

   A service provider offers pay-per-use services. A user should be registered with the service provider in order to access a service. Registration is required for first-time users only. Moreover, users can access a service only if they have sufficient credit. There can be only 10 simultaneous usages of the same service.

4. **(1 point)** Describe the EPAL policy model.

5. **(1.5 points)** Consider the RT framework.

   (a) Consider the following situation: Alice, Bob and Charlie decide to set up a music club to share their music interest. Each club member provides definitions for the role names name .music and .favoritemusic, so that they can know from each other which music they have (.music) and which music they particularly like (.favoritemusic). Now, David joins the group, and defines his own roles David.music and David.favoritemusic. In addition, David defines the new role David.worthlistening which is the RT translation of the following policy: if either Alice, Bob or Charlie likes a certain piece of music, then David declares it as worth listening to. Write a definition for this role, using a linked role.

(b) Now David defines the role David.veryworthlistening, which is the RT translation of the following policy: if any two of Alice, Bob and Charlie like the same piece of music, then David declares it as very worth listening to. Write a definition for this role.

(c) Later, also Ellen joins the club, and David wants to change the definition of the role David.veryworthlistening to take into consideration also Ellens tastes as follows: if any two of Alice, Bob. Charlie and Ellen like the same piece of music, then David declares it as very worth listening to. Write a definition for this role.

(d) Is it possible to make sure that the definition given in (c) looks the same as the definition in (b) and that it scales up also when other people will join the club? Motivate your answer.

(e) Consider the following RT_0 Policy.
$A.r \longleftarrow B.r \cup D.t$
$B.r \longleftarrow B.s.t$
$B.s \longleftarrow A.r$
$B.s \longleftarrow C.t$
$C.t \longleftarrow D$
$C.t \longleftarrow E$
$C.t \longleftarrow F$
$D.t \longleftarrow C$
$D.t \longleftarrow G$
Assume that the top level query is "find all principals populating $A.r$" (which means, compute $[[A.r]]$). Write down the graph generated by the top-down algorithm when computing the semantics of $A.r$. (the top-down algorithm is also known as the "backward algorithm").

6. **(1 point)** What are the security mechanism to protect data confidentiality at transport layer (communication channel) and which mechanisms are used at the application layer (e.g. for document protection)? What is granularity of encryption that can be achieved using XML encryption and which key management methods it supports?

7. **(1.5 points)** Given the XACML policy and access request below, determine the access response.
Hint: If an attribute from the request context does not match the target of the Rule/Policy/PolicySet, then the attribute is considered missing. If the attribute is missing, then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

- If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
- If MustBePresent is "True", then a missing attribute results in "Indeterminate".

Access Request

```
  <Request>
    <Subject>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
            Alice
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
            manager
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
            accountant
        </AttributeValue>
      </Attribute>
     </Subject>
     <Resource>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
           financialrecord
        </AttributeValue>
      </Attribute>
    </Resource>
    <Action>
      <Attribute
         AttributeId="urn:oasis:names:tc:xacml:2.0:subject:action-id"
         DataType="http://www.w3.org/2001/XMLSchema#string">
       <AttributeValue>
           read
       </AttributeValue>
      </Attribute>
    </Action>
    <Environment/>
  </Request>
```

```
<PolicySet PolicySetId="PS"
    xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides">
  <Target>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
          <ActionAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true" />
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
  <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">financialrecord</AttributeValue>
            <ResourceAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
    <Rule Effect="Deny" RuleId="R1">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#time">08:00</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time"
                  MustBePresent="true" />
            </SubjectMatch>
          </Subject>
        </Subjects>
```

```
    </Target>
  </Rule>
  <Rule Effect="Deny" RuleId="R2">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
    </Target>
  </Rule>
  <Rule Effect="Permit" RuleId="R3">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
```

```
  <Policy PolicyId="P2"
     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
    <Target />
    <Rule Effect="Deny" RuleId="R4">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    </Rule>
    <Rule Effect="Permit" RuleId="R5">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">08:00</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```